State of Montana Information Security Advisory Council

Council Meeting Minutes
April 21, 2016
1:00 p.m.
Capitol Building – Room 350

Members Present:

Bryan Costigan, MATIC
John Daugherty, COR
Joe Frohlich, SITSD
Kreh Germaine, DNRC
Jim Gietzen, OPI
Margaret Kauska, DOR
Lynne Pizzini, CISO, Acting Chair
Maj. Gen. Matthew Quinn, DMA
Dawn Temple, DOJ
🖱 Erika Billiet, City of Kalispell
🖱 Adrian Irish, UM

Staff Present:

Jennifer Schofield
Tim Wunderwald
Noah Horan

Guests Present:

Rebecca Cooper, Bryan Fox, Mike Mazanec, Suzi Kruger, John Burrell, Lance Wetzel, Tim Kosena, Eric Durkin, Craig Stewart

🖱 Real-time Communication:

Michael Barbere, Kyle Belcher, Phillip English, Brad Flath, Michael Jares, Anne Kane, Jerry Kozak, Darrin McLean, Christi Mock, Rawlin Richardson, Angie Riley, Ed Sivils, Lisa Vasa, James Zito

Welcome and Introductions

Lynne Pizzini welcomed the council to the April 21, 2016 MT-ISAC meeting. All members and guests were introduced.

Minutes

The council reviewed the March 17, 2016 Minutes. Dawn Temple noted that the level of specificity employed in the University Incidents overview was unnecessary. The council adopted the Minutes as amended.

Business

Time Change for MT-ISAC Meetings

Lynne mentioned that MT-ISAC's scheduled time is changing to avoid conflict with the 9-1-1 Advisory Council. MT-ISAC meetings will now be held from 11 a.m. to 1 p.m. on the third Thursday of each month, beginning in May.

First Governor's Dashboard

The first Dashboard was presented to the Governor's Office in April. It is a confidential document. It is posted on SharePoint, and is available for viewing by any members of the council.

MT-ISAC Review of Accomplishments

Joe Frohlich provided an overview of the MT-ISAC Review of Accomplishments document, which is available on the MT-ISAC website. The document is a scorecard outlining workgroup progress towards meeting pre-established objectives. 37 total objectives were set by MT-ISAC in August 2015. Five were approved as accomplished in January 2016, seven are currently being worked on, and six are proposed for the council to approve as accomplished.

Q: Bryan Costigan: If a workgroup finalizes a project as a best practice, will it be moved to the best practices workgroup?

A: Joe: Workgroups can collaborate on goals and projects.

A: Lynne Pizzini: If we feel that we need a workgroup to work on a particular best practice, we will assign it accordingly.

Maj. Gen. Quinn has spoken with Missoula College about offering an Associate's Degree program in information security. Missoula College anticipates receiving accreditation this fall, but the date may be pushed back due to funding issues. The President's Initiative may provide funding.

Q: Bryan Costigan: How broad will the two-year program be? Will it include investigative training?

A: Maj. Gen. Quinn: Part of this program will include forensics. The goal is to educate and train credentialed, degreed individuals that would go through a structured program.

Lynne: In the future, we can expand this goal to cover a broader range of topics. The original objective was to create a formalized two-year degree program due to the need for such a program.

Maj. Gen. Quinn: A four-year degree program should be explored in the future. The Department of Homeland Security offers a scholarship program where, if an individual graduates with an information security degree and goes to work for city, county, tribal, state, or federal government, they can get their college paid for.

Q: Adrian Irish (via Skype): I would like to see a Master's track for Computer Science. Who did you talk with regarding this?

Maj. Gen. Quinn: We did not discuss a Master's program. I spoke with President Royce Engstrom at the University of Montana, and with Dean Shannon O'Brien at Missoula College.

Joe Frohlich provided an overview of the six objectives proposed for approval as accomplished. There was a discussion regarding the Situational Awareness workgroup's goal of enhancing situational awareness within state government. Dawn Temple mentioned that the Tools workgroup would like more information out of other workgroups. Agencies would like more substantive information included in monthly incident reports. Sean Rivera mentioned that SITSD often does not get back specific details from agencies regarding infections and incidents. Lynne mentioned that the Situational Awareness workgroup needs to document its activities before its goals can be considered "accomplished."

Q: Maj. Gen. Quinn: What does it mean when we say that we have accomplished something that is still ongoing?

A: Lynne Pizzini: We are saying that we now have a process in place, which can be used in an ongoing capacity.

Q: Kreh Germaine: Could we use the word "addressed" instead of "accomplished?"

Maj. Gen. Quinn: I like addressed and ongoing. We could have multiple criteria, such as: tasks that are accomplished; tasks that are addressed and ongoing; and tasks that are not yet addressed.

A: Lynne: It is important to realize that it is not that the objective is done, but that there is something in place that is continuing to address the objective.

Jim Gietzen: We need to be continuing to talk to these groups on a regular basis.

Kreh: We need feedback from these groups before we can say we have accomplished a goal. Have we covered the channels, and are people getting the info they need?

Joe: Our focus is government, so we have identified those channels. We have looked at K-12. This list can grow to include outreach to the public. It is never going to be accomplished as in "finalized," but rather is an ongoing process.

Lynne: We will defer the vote. Please review the process and come to the next meeting with suggestions.

Workgroup Updates

Assessment Workgroup Update

Lynne updated the council on the Assessment workgroup's several objectives. The workgroup has been working on the Assessment document. It has been out for review on the MT-ISAC website. The workgroup asks that the council votes to accept this document.

Q: Kreh Germaine: If the council accepts the Assessment document, will it be optional or required?

A: Lynne: This will be a required report. It is intended to standardize assessment practices across all agencies.

Q: Maj. Gen. Quinn: What if we made this a best practice assessment tool instead of a mandated reporting tool?

A: Lynne: One of our agreed-upon objectives as a council was that we needed an assessment tool. The Assessment workgroup decided that this tool is the best method. SITSD will fill out part of this tool for you, because we are responsible for the network. HB 10 provides funding to contract for services to help with the enterprise security program.

Bryan Costigan: We should try this assessment as a pilot with a specific agency to see how it goes.

Lynne: Great idea.

Philip English (via Skype): In healthcare, these kind of assessments are mandatory. Most entities utilized both the self-assessments and outside auditing services.

Best Practices Workgroup Update

Lynne spoke on the Technical Small Cyber Incident Handling document that the council reviewed prior to the meeting.

Q: Dawn: Should we really reimage an infected machine right away? Shouldn't we collect information first?

A: Lynne: We will restate the point and add something regarding doing discovery on the device before reimaging.
A: Sean: There is room for interpretation regarding when it is appropriate to reimage a machine.
Q: Kreh: Is there a step for salvaging critical information from an infected device?
A: Joe Frohlich: That was not discussed because it is best practice not to store documents locally on the device. Documents should be on the server or in the cloud.
Dawn: We have users who work offline. Montana Highway Patrol often saves things locally. We have safe ways of recovering critical files without booting to the OS.
Lynne: Best Practices workgroup will modify the document and upload it to the MT-ISAC website for review again.

Lynne: The workgroup is also reviewing Large Incident Handling processing. We are working on sanitation and disposal of devices. We are collecting information on encryption best practices, vulnerabilities and patch management best practices, and user ID and authentication best practices.

Situational Awareness Workgroup Update
Bryan Costigan: We have been focusing on internal situational awareness.

Tools Workgroup Update
Dawn: Joe Frohlich asked us to focus on antivirus strategy issues. Microsoft is offering phone time with a Premier Field Engineer (PFE) on April 28, 2016 from 1 to 3 p.m., who will be available to troubleshoot Endpoint Protection. The group is working on an advanced endpoint strategy. The group is also working on hardening of devices, including preliminary assessments with each agency.
Lynne: The Device Hardening strategy is a best practice. You must follow the strategy to be in compliance with the policy. The Device Hardening strategy needs to go back to the Best Practices workgroup in regards to the requirement versus recommendation concerns.

Current Threats

Sean gave an update on current threats, including a summary of a 60 Minutes blurb called "Hacking Your Phone." Two security experts were interviewed, who demonstrated the ease of intercepting email and compromising a phone. This is accomplished via Signaling System 7 (SS7), a global system that connects all cellular data providers. Via SS7, hackers are able to track a phone via GPS and intercept phone calls. It also allows for the compromise of cell phone-based two-factor authentication tokens.

Sean also mentioned that QuickTime for Windows is no longer supported by Apple. There are two critical vulnerabilities in place, and Apple has abandoned the software rather than update it to fix these vulnerabilities. All agencies are advised to remove QuickTime from their devices.

Adjournment

Next Meeting
Thursday, May 19, 2016, State Capitol, Room 137

Open Forum
Lynne Pizzini: The IRS is going to be conducting their audit during the week of April 25, 2016.
John Daugherty: We are hiring a new Information Security Manager (ISM). We will be posting the job listing soon.

Public Comment
None.

Adjourn
The meeting adjourned at 2:45 p.m.

Adopted May 19, 2016.